REMARKS

Reconsideration and further examination is respectfully requested.

The Examiner is thanked for the careful consideration of Applicants' previous remarks, and the additional description of the Examiner's analysis. Applicants believe that the below remarks support the Applicants' continued belief in the novelty of the claims in view of the combination o Mittra and He.

Rejections under 35 U.S.C. §103

Claims 1-8, 10-25, 27-28, 31-45, 47-61, 63-75, 77-87, 89-105, 108-128, 131-145 and 149 were rejected under 35 U.S.C. §103(a) as being unpatentable over Mittra, U.S. Patent 5,748,736 in view of He.

Mittra:

Mittra describes at column 7, lines 45-65:

"…Joining a secure multicast group requires the joining member first to set up a separate secure channel with the GSC of the group (using a unicast communication line). The purpose of the secure channel is to facilitate and isolate confidential communication between the GSC and this member during the time that the member is part of the group… Upon receiving a join request (and approving it), the GSC inserts the member's identification and information concerning the secure channel in a private database it maintains. In this way the GSC has full knowledge of the group membership and can communicate with each member separately and securely when required. The member must also store information concerning the secure channel for future communication with the GSC… All communications from the GSC must include a message digest and be digitally signed so that receivers may verify that the message has not been corrupted and the sender was actually the GSC… Only the GSC maintains information concerning group membership; members do not know about each other (except that receivers may need to know the list of authorized senders)…" …"

Mittra also states, at column 8, lines 14-22:

"…Once the GSC and the new member have authenticated each other and have agreed on a secret the GSC needs to provide the new member with information that will allow it to encrypt and/or decrypt the multicast transmission. At this point the GSC also needs to change the group

key (Kgrp) which provides access to the multicast transmissions. This is done to prevent the joining member from decrypting previous transmissions to which it should not have access…"

Thus, in Mittra, when a device seeks to join a group:

1). The host establishes a separate side channel communication with the GSC.
2). Within the channel, the host issues a 'join request' to the GSC start authentication. In response to the 'join' request, the GSC starts the authentication process
3). When authenticated, the host receives a group key from the GSC
4). The host communicates within the group.

Mittra does not go in to detail about how the host is authenticated at the GSC. However, once it is authenticated, it receives a key. There is no mention in Mittra that the host receives an 'access token' as recited in the claims of the present invention.

He:

He describes a system and method for securing access to network elements by user elements. He states "...an authentication server responsible for authentication of the network users to network elements, a credential server responsible for controlling the network user credentials or privileges, and a network element access server responsible for controlling of access to the network elements by the user elements. A registration database facilitates administration and management of access to the network by the user elements..." (Abstract)

He describes at column 8, lines 42-47:

"...User authentication is accomplished through the establishment of the so-called "secret password" for each user identifier. (The term "secret password," however, has many synonyms, such as secret key, private key, private password, or the like. It is more accurate, and worth noting, that the word "password" connotes the human readable form of a "secret password," and the word "key" refers to a computer readable form, internal representation or mapping of the "password."..."

At column 9, lines 37-42, He describes:

"...User access authorization is accomplished through the establishment of an access control list for each network resource or information. This list shall contain the list of user identifiers who are allowed to access it and the kind of access rights that are allowed to each user. The access control list can also be established based on user identities that specify the list of network resources and information the user is allowed to access along with the exact access rights or the kind of operations the user is allowed to perform on the network resources and information..."

Accordingly, when contemplating user authentication, He describes the use of a user access control list that includes member identifiers.

Applicants note that the limitation of the 'access token' which includes 'a token identifier' has been amended to include the limitation that the access token includes a host identifier. Applicant's access token is an element which clearly distinguishes over the Mittra and He art; in the present invention an access token is provided by a key server, and distributed to the host and to the access devices. The access token thus is a unique token that is used to authorize the host's ability to join the multicast tree at the access device. The system of Mittra includes both key distribution and access point at a common server... thus there is no need in Mittra for an access token such as that of the claimed invention. As highlighted in some of the dependent claims of the present application, the access token may have associated therewith an expiration date, thereby limiting the amount of time that a host may be able to join a multicast group. The access token is therefore unique to the host/group information pair, allowing the host to access a particular group.

The Examiner states, at page 32 of the office action:

"...The primary concern addressed within the amendment is the amended independent claim trait of "the authentication information including an access token comprising a token identifier and an authentication key for authenticating the host with the designated device." This claim trait is essentially that of the now cancelled claim 9. The addition of claim 9 into the

independent claims however does not overcome the prior art. It is known in the art that during authentication, the access information must contain an id of some form to distinguish it; hence a token identifier inherently must be present. Mittra discloses the use of a member id that is equivalent to the claimed token identifier (column 7, lines 52-54). In addition, keys are present in Mittra's design and are deemed equivalent to the authentication keys..."

Applicants first note that the Examiner's reasoning that a member id is equivalent to the language of the claims does not give patentable weight to the claim language which describes that the access information is unique to the host/group pair; a member ID is not unique to a host group par. However, to further clarify distinctions between the art and present invention, Applicant has amended the claim to more particularly distinguish a token identifier from a membership id, to highlight the fact that it is the particular *token* that is used to verify the authorization of the host to going the group. Thus, there is a token identifier associated with a host identifier... both are now included in the claim, and it is respectfully noted that such a function or feature is neither shown nor suggested by Mittra, He or the combination thereof.

As described in M.P.E.P. §2143, "To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations" The combination of Mittra and He fails to satisfy this burden for at least the following reasons.

No motivation for the modification suggested by the Examiner

Although the Examiner states that Mittra would be motivated to provide separate authentication and access control "to effectively provide security mechanisms," Applicants note

that there is a fundamental difference in controlling access to multicast groups, with frequent changes in membership, and controlling access to resources. Accordingly, methods used by one, such as having separate servers for controlling access to elements, may cause delays that would serve to frustrate operation of maintaining up to date multi-cast groups.

Combination neither describes nor suggests an 'access token' comprising a 'token identifier' that is 'unique to the host/group pair'

Independent claims 1, 16, 28, 40, 61, 68, 75, 87, 99, 122, 145

Assuming that a motivation could be found for the combination suggested by the Examiner, Applicants note that the independent claims have each been amended to clearly distinguish the present invention from a system which maintains a user identifier, to one that has an 'access token' unique to the host/group pair. Each has been amended to include the limitation "...wherein the authentication information including an access token comprising *a host identifier, a token identifier and an authentication key* for authenticating the host with the designated device" and "wherein the authentication is unique to the host/group pair." No such feature is shown or suggested in the combination of Mittra and He. In the present invention, the access token is for a particular host and provides access to a particular multicast group. . The host obtains a different access token for each multicast group that it joins. This token is delivered to the host, and to the designated router, so that requests to join a multicast group may be authenticated by the designated router. Mittra, which has a centralized controller, would have no need for such a token.

Although when the Examiner is describing Mittra he states that 'the access information must contain an id of some form to distinguish it' there is no mention or suggestion in Mittra that

there is anything but a key associated with a group, or a host identifier associated with a host. Thus there is not teaching or suggestion in Mittra that there is an 'id' associated with the 'access information', where the 'id' is *unique to the host/group pair*. Rather, in Mittra, the 'id' is the key number., or the group member identifier. Accordingly, for at least the reason that the combination of references fails to describe or suggest the invention as recited in each of the independent claims, it is respectfully requested that the rejection be withdrawn.

As stated in M.P.E.P. §2143.03 " If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)..." Accordingly, for at least this reason, the dependent claims of this application are also patentable over the combination of Mittra and He, and it is requested that the rejection be withdrawn.

Conclusion

Applicants have made a diligent effort to respond to the request for information. However, should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone Lindsay G. McGuinness, Applicants' Attorney at 978-264-6664 so that such issues may be resolved as expeditiously as possible.

Respectfully Submitted,

5/9/2007
Date

_/Lindsay mcGuinness/_____
Lindsay G. McGuinness, Reg. No. 38,549
Attorney/Agent for Applicant(s)
McGuinness & Manaras LLP
125 Nagog Park Drive
Acton, MA 01720
(978) 264-6664

Docket No. 120-147